MEMORANDUM OF UNDERSTANDING
between
UNIVERSITY OF TENNESSEE
and
THE TENNESSEE DEPARTMENT OF HEALTH
For the Study of
The Dynamics of Prescription Opioids, Job Separation, and Employment Stability

1.0 PURPOSE

The purpose of this Memorandum of Understanding ("MOU") is to develop academic and educational cooperation in understanding the economic impact of opioid use in the labor market for the benefit of the people of Tennessee through the Tennessee Department of Health (hereinafter referred to as "TDH" or the "State") and The University of Tennessee on behalf of its Boyd Center for Business and Economic Research ("BCBER"). Both BCBER and the TDH may be referred to individually as a "Party" or collectively as the "Parties."

2.0 SCOPE OF ACTIVITIES

2.1 The TDH Controlled Substance Monitoring Database ("CSMD") Committee has approved BCBER's use of individual level data from the CSMD ("CSMD Data") in the performance of the study "The Dynamics of Prescription Opioids, Job Separation, and Employment Stability" ("Research") as outlined in and attached hereto as Exhibit 1. This shall be a one-time data share.

2.2. BCBER shall use the following data to perform the Research:

2.2.1. CSMD Data, provided by TDH hereunder;

2.2.2. Employment and wage data from the Tennessee's longitudinal database system ("P20 Connect"), as available to BCBER independently.

2.3 BCBER research personnel ("Research Personnel") shall include but not be limited to:

2.3.1. Tammy Lemon, Director, and Tom Jenkins, Assistant Director, P20 Connect, Boyd Center for Business and Economic Research, University of Tennessee for the purposes of receiving the CSMD Data in a secure method, matching to P20 Connect data and providing investigator Research Personnel with a masked dataset that does not include personally identifiable information such as name and social security number; and

2.3.2. Matthew C. Harris, Ph.D., Assistant Professor, Department of Economics and Boyd Center for Business and Economic Research, University of Tennessee is the primary investigator and responsible for oversight of the Research Personnel required to complete the Research.

2.4. BCBER shall share the results of the Research with TDH, including but not limited to:

2.4.1. a white paper from both the descriptive and causal results;

2.4.2. an academic research paper targeted towards an economics journal; and/or

2.4.3. partner with TDH personnel on projects related to the economic impact of opioid use.

3.0 RESPONSIBILITIES OF THE PARTIES

3.1 General responsibilities

3.1.1. TDH shall provide the CSMD Data to BCBER through a mutually agreeable, secure method.

3.1.2. BCBER shall maintain the CSMD Data in a secure manner.

a. Security Standards: P20 Connect employs physical, electronic, operational, and procedural security controls based on national standards for security controls published by the National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev4. The use of these security controls in mandated for Federal agencies by Federal Information Processing Standards (FIPS) 199.

b. Physical System Security: P20 Connect servers are maintained in a secured server room to restrict physical access and ensure only authorized personnel are able to gain entry. In addition, firewall protection and intrusion detection efforts are in place for the system components. All CSMD data will be encrypted at rest.

c. Access Security: BCBER P20 Connect staff are responsible for enabling Research Personnel authentication and authorization to the CSMD data as permitted by TDH.

d. Data Transport Security: All data transfers are encrypted. Source data files with personally identifiable information are stored in a secured location with access limited to P20 Connect staff.

3.1.3. CSMD Data is highly sensitive and confidential information, and BCBER shall restrict access to the CSMD Data to only those Research Personnel authorized by TDH. Research Personnel are required to comply with all applicable state and federal laws, and policies, procedures, and requirements of the Research, including, without limitation, those related to confidentiality, privacy and security of patient/client records, and patient/client information. All work undertaken by Research Personnel on identifiable data shall take place on the premises of BCBER, and under no circumstances shall the Research Personnel remove any identifiable CSMD Data, whether in hard copy or electronic medium, from the premises of BCBER. Any violation of this provision shall be, at the discretion of TDH, grounds for immediate termination of this MOU. TDH confidentiality requirements survive the completion of the Research and the expiration or termination of this MOU.

3.1.4. Each Research Personnel that will access CSMD Data shall complete and return a CSMD data use form and return it to TDH prior to accessing any CSMD Data.

3.1.5. BCBER represents to TDH that Research Personnel participating in the Research are not:

a. currently excluded, debarred, or otherwise ineligible to participate in the Federal health care programs as defined in 42 U.S.C. Section 1320a-7b(f) (the "Federal health care programs");

b. convicted of a criminal offense related to the provision of health care items or services;

c. under investigation or otherwise aware of any circumstances which may result in BCBER or Research Personnel being excluded from participation in the Federal health care programs;

d. convicted felons;

e. sexual offenders; or

f. elder abuse offenders.

3.1.6. Each Party shall be solely liable for payment of its portion of all claims, liability, costs, expenses, demands, settlements, or judgments resulting from negligence, actions or omissions of itself or those for whom it is legally responsible relating to or arising under this Agreement. Any and all monetary claims against the State of Tennessee or The University of Tennessee, or their respective officers, agents, and employees in performing any responsibility specifically required under the terms of this Agreement shall be submitted to the Board of Claims or the Claims Commission of the State of Tennessee and shall be limited to those provided for in T.C.A.§ 9-8-307.

3.1.7. HIPAA Compliance. TDH and BCBER shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH") Act and any other relevant laws and regulations regarding privacy (collectively the "Privacy Rules"). The obligations set forth in this Section shall survive the termination of this MOU.

a. BCBER represents to TDH that it is familiar with the requirements of the Privacy Rules, and will comply with all applicable requirements in the course of this MOU.

b. BCBER represents that it will cooperate with TDH, including cooperation and coordination with State privacy officials and other compliance officers required by the Privacy Rules, in the course of performance of the MOU so that both parties will be in compliance with the Privacy Rules.

c. TDH and BCBER will sign documents, including but not limited to business associate agreements, as required by the Privacy Rules and that are reasonably necessary to keep TDH and BCBER in compliance with the Privacy Rules. This provision shall not apply if information received or delivered by the parties under this MOU is NOT "protected health information" as defined by the Privacy Rules, or if the Privacy Rules permit the parties to receive or deliver the information without entering into a business associate agreement or signing another document.

3.1.8. Confidential State Data.

a. "Confidential State Data" is defined as data deemed confidential by State or Federal statute or regulation. BCBER shall protect Confidential State Data as follows:

(1) BCBER shall ensure that all Confidential State Data is housed in the continental United States, inclusive of backup data.

(2) BCBER will receive CSMD data with personally identifiable information as specified in paragraph 3.1.3. The personally identifiable portion of the data will be used to match with other data within the P20 Connect Data Warehouse. Once the matching is completed a separate copy of the data will be generated with a unique identifier substituted for the identifiable data. The Unique identifier will be maintained with the personally data for tracking purposes. BCBER shall encrypt the CSMD data set including this unique identifier at rest and in transit using the current version of Federal Information Processing Standard ("FIPS") 140-2 validated encryption technologies. The data set with the substituted unique identifier and the linked P20 Connect data will not be encrypted but will be

contained in the secure P20 Connect warehouse for analysis. The only persons with access to the linked data set are BCBER administrators (identified above) and approved BCBER Researchers.

(3) BCBER and the BCBER's processing environment containing Confidential State Data shall either (1) be in accordance with at least one of the following security standards: (i) International Standards Organization ("ISO") 27001; (ii) Federal Risk and Authorization Management Program ("FedRAMP"); (iii) National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4; or (2) be subject to an annual engagement by a CPA firm in accordance with the standards of the American Institute of Certified Public Accountants ("AICPA") for a System and Organization Controls for service organizations ("SOC") Type II audit. The State shall approve the SOC audit control objectives. The Contractor shall provide proof of current ISO certification or FedRAMP authorization for the Contractor and Subcontractor(s), or provide the State with the Contractor's and Subcontractor's annual SOC Type II audit report within 30 days from when the CPA firm provides the audit report to the Contractor or Subcontractor. The Contractor shall submit corrective action plans to the State for any issues included in the audit report within 30 days after the CPA firm provides the audit report to the Contractor or Subcontractor.
If the scope of the most recent SOC audit report does not include all of the current State fiscal year, upon request from the State, the Contractor must provide to the State a letter from the Contractor or Subcontractor stating whether the Contractor or Subcontractor made any material changes to their control environment since the prior audit and, if so, whether the changes, in the opinion of the Contractor or Subcontractor, would negatively affect the auditor's opinion in the most recent audit report. No additional funding shall be allocated for these certifications, authorizations, or audits as these are included in the Maximum Liability of this Contract.

(4) BCBER and all data centers used by BCBER to host State data, including those of all Subcontractors, must comply with the State's Enterprise Information Security Policies as amended periodically or the equivalent University of Tennessee Security Policy, whichever is more stringent. The State's Enterprise Information Security Policies document is found at the following URL: https://www.tn.gov/finance/strategic-technology-solutions/strategic-technology-solutions/sts-security-policies.html. The University's Security Policies can be found at the following URL: https://oit.utk.edu/security/policies-procedures/.

(5) In the event that the operating system is an integral part of the application, BCBER agrees to maintain Operating Systems at current, manufacturer supported versions. "Operating System" shall mean the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.

(6) BCBER agrees to maintain the Application so that it will run on a current, manufacturer-supported Operating System. "Application" shall mean the computer code that supports and accomplishes the State's requirements as set forth in this MOU. BCBER shall make sure that the Application is at all times fully compatible with a manufacturer-supported Operating System; the State shall not be required to run an Operating System that is no longer supported by the manufacturer.

(7) If the Application requires middleware or database software, BCBER shall maintain middleware and database software versions that are at all times fully compatible with current versions of the Operating System and Application, to

ensure that security vulnerabilities are not introduced.

(8) BCBER will annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment. “Processing Environment” shall mean the combination of software and hardware on which the Application runs. “Penetration Tests” shall be in the form of software attacks on BCBER’s computer system, with the purpose of discovering security weaknesses, and potentially gaining access to the computer's features and data. The “Vulnerability Assessment” shall have the goal of defining, identifying, and classifying the security holes (vulnerabilities) in BCBER’s computer, network, or communications infrastructure.

P20 Connect will conduct annual penetration tests addressing the following assessments:

Areas of Penetration Test

- External Network Assessment
- Internal Network Assessment
- Phishing
- Physical Security
- Social Networking

Penetration Test Methodology

- Information Gathering – Reconnaissance on a target; this includes publicly available information on systems, people, and processes.
- Network Mapping – Discovering live hosts, open ports, operating systems, available services, firewall rules, and enumerating network topology.
- Vulnerability Identification – Using automated and manual tools to determine system weaknesses. Perform false positive reduction and estimate probable impact of exploitation. Identify available attack paths.
- Gaining Access by Penetration & Exploitation – Gain unauthorized access to the system using attack tools and techniques.
- Privilege Escalation – Attempt to achieve the highest access possible for a system, typically administrative control.
- Expand Control & Foothold – Infiltrate the target network, using discovered information and elevated access to gain control of as many new systems as possible in the target environment.
- Pilfer Sensitive Data – Show valid access to sensitive data in an environment. UTK testers will not perform an exhaustive exfiltration of data. The testers will access the minimum amount of sensitive data possible to demonstrate compromise.

b. Business Continuity Requirements. BCBER will maintain regular up-to-date backups of the research data and the CSMD. Should an incident occur to interrupt business operations, the P20 Connect data warehouse will be returned to operations as soon as practical.

c. Upon State request, BCBER shall provide a copy of all Confidential State Data it holds. BCBER shall provide such data on media and in a format determined by the State.

d. Upon termination of this MOU and in consultation with the State, BCBER shall destroy all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology ("NIST") Special Publication 800-88. BCBER shall provide a written confirmation of destruction to the State within ten (10) business days after destruction. The CSMD Data received hereunder may be retained by BCBER no longer than 180 days after the termination of this MOU.

3.2. Detailed management of intellectual property rights and publications

3.2.1. BCBER shall seek the appropriate Institutional Review Board ("IRB") approvals for the Research. TDH's IRB Committee is available as the mechanism for reviewing and recommending for approval research projects.

3.2.2. TDH's Institutional Review Board (IRB) Committee is available as the mechanism for reviewing and recommending for approval research projects, including those initiated by either Party.

3.2.3. Authorship on papers and manuscripts derived from the work will be determined in accordance with the criteria set forth by the International Committee of Medical Journal Editors. Regardless of authorship, TDH will be provided the opportunity to review and comment on manuscripts prior to submission and publication, and will be notified of all accepted manuscripts and publication dates before publication.

3.3. Disposition of Data

3.3.1. CSMD Data that is retained after the termination of the Research must be maintained in a secure method as described in Section 3.1.2 above.

3.3.2. Any additional research that BCBER proposes to perform with CSMD Data must be approved by the CSMD Committee, receive the appropriate IRB approvals, and shall be subject to a separate agreement regarding that particular research. Access to CSMD Data shall remain restricted to only those BCBER personnel who have been approved by TDH and have submitted a CSMD data use form described in Section 3.1.4 above.

4.0 RENEWAL, TERMINATION, AND AMENDMENT

4.1. This MOU shall remain in force for a period of three (3) years from the date of the last signature. This MOU may be extended by the written consent of the Parties

4.2. This MOU may be terminated by either Party upon thirty (30) days advance written notice.

4.3. This MOU may be reviewed annually by the Parties in order to address issues identified by either Party to this MOU. This MOU may be amended only by the written consent signed by the Parties.

IN WITNESS WHEREOF, the Parties have offered their signatures hereto:

UNIVERSITY OF TENNESSEE:

CHRIS CIMINO, SENIOR VICE CHANCELLOR **DATE**

TENNESSEE DEPARTMENT OF HEALTH:

Lisa Piercey MD-LO

Digitally signed by Lisa Piercey MD-LO
DN: cn=Lisa Piercey MD-LO, o, ou, email=Lindsay.R.Oliveras@tn.gov, c=US
Date: 2019.09.12 09:36:07 -05'00'

LISA PIERCEY, MD, MBA, FAAP, COMMISSIONER **DATE**

EXHIBIT 1
RESEARCH PROTOCOL

The Dynamics of Prescription Opioids, Job Separation and Employment Stability

Matt Harris
Larry Kessler
Matthew N. Murray

Boyd Center for Business and Economic Research
The University of Tennessee, Knoxville

Background

Use of prescription opioids has sharply increased across the United States, but particularly in Tennessee. A 2015 report showed that over 50% of publicly-funded substance abuse treatment admissions in Tennessee were attributable to opioids, compared to a 16% national average. In addition, 4.56% of the population of Tennessee was classified as addicts or risky users in need of early intervention. Among young people (aged 18-25), the rate of use of prescription opioids was 30% higher in Tennessee than the national average.

The scope of the prescription opioid epidemic and the public health costs associated with increased prescription opioid use are increasingly well understood. The full *economic* costs of increased prescription opioid use to individuals and society remain largely unknown. In a working paper currently under review at a peer-reviewed journal, we found evidence that increased opioid prescriptions per capita at the county level led to decreased labor force participation rates and higher rates of unemployment. These findings have important implications for understanding economic development patterns across the state in both rural and urban settings and helps motivate a call to action on the part of society and policymakers.

However, we believe that understanding the dynamics at the individual level is of equal or greater value to the State of Tennessee. To the extent that prescription opioid use affects an individual's expected future income, prescription opioid use is a social determinant of expected future health and wellbeing as well. Also, understanding the impact of prescription opioid use on individual's labor market outcomes will allow a better of understanding of the implications for economic and community development. If prescription opioid use affects the availability of workers and expected workplace productivity, allocating additional funds for preventing opioid use may positively affect Tennessee's expected future economic growth.

Finally, job loss or decreased employment stability are easily observable markers that indicate an individual may be losing control over their life. To the extent that we can link individuals' prescription patterns to decreased employment stability in subsequent

periods, our research may yield benchmark thresholds for early intervention.

Data

The primary data for this study will come from two sources. Employment and wage data will come from Tennessee's unemployment insurance administrative records and unemployment claims. These data are provided by the Tennessee Department of Labor and Workforce Development and are housed in the Tennessee P20 Connect database (formerly referred to as the Tennessee Longitudinal Database System or TLDS) maintained by the Boyd Center. Data on opioid prescriptions will come from Tennessee's Controlled Substance Monitoring Database (CSMD), administered by the Tennessee Department of Health (TDH). This section describes the relevant fields from each data source, both for the research analysis and for merging data from each source at the individual-quarter level.

Employment and Unemployment Data

The vast majority of workers in Tennessee are covered under the state's unemployment insurance (UI) program. Each quarter, employers report wages paid for all employees in Tennessee. From these data, we are able to identify (i) individuals who are currently employed in a given quarter and (ii) the wages they have earned in each quarter since 1996. From the same UI system, we also have data on all unemployment claims, meaning we can identify workers who have been displaced from a given job. Therefore if a person is not visible in the UI data, they are either out of the labor force or are probably employed in a sector of the labor market that operates outside the UI system. The relevant fields from the employment data from the UI system include:

☐ Whether an individual is employed in a quarter

☐ The individual's wages, conditional on employment

☐ Tenure with employer

☐ Whether the individual has been terminated/displaced from a job

☐ Duration of unemployment spell

☐ Number of employers in a given time period (quarter/year)

If prescription opioid use affects an individual's performance in the workplace, each of the above variables can provide insight on the effect of opioids on the individual's employment prospects—each measure is an important metric of labor market engagement and performance.

Data on Prescription Opioids

From the Data Dictionary provided by TDH and CSMD, we seek the following fields for all opioid prescriptions available after such a time that CSMD is confident in the quality of the data (2014?-present):

- Prescription information: DrugID, Drug, DEASchedule, Strength, Product, Form, DEAClass, DEAClassCode, Class of Drug, StrengthPerUnit, UnitOfMeasure, MMEConversion Factor, DateFilled, DatePrescriptionWritten, DateSold, DaysSupply, NumberOfAuthorized Refills, PartialRefill, PatientID, PractitionerID, Pharmacy ID, Quantity.
- Patient Information: City, CountyFips, DateOfBirth, FirstName, Gender, LastName, MiddleName, PatientID, Species, Street, Street2, State, Zip.
- Pharmacy Information: Street, City, State, Zip, CountyFIPS, Pharmacy Name,
- Practitioner Information: Practitioner Name, Practitioner ID, FirstName, MiddleName, LastName, Street, City, State, Zip, Is Dispensing, ICD9, ICD10.

The need for patient data is self-evident for both forming individual prescription histories and for merging with the labor market data. It is our understanding that SSN's are not available for patients in the CSMD. However, P20 Connect has implemented algorithms to match individuals based on hand-keyed names, date of birth, and where available, location data, across databases from the UI system, Department of Education (DoE), and Tennessee Higher Education Commission (THEC). While accessing data from DoE and THEC is outside the bounds of the immediate study, data from these other domains can be useful in triangulating uniquely identifiable individuals. The physician and pharmacy data are also invaluable from an empirical standpoint as identifiers of *causal effects*.

Research Methodology

Using contextual data from other domains in the P20 Connect, we will define the unit of observation as a person-quarter as we seek to identify the effects of opioids on individual labor market outcomes. The primary empirical analysis will consist of panel-data regressions, which will incorporate instrumental variables approaches and dynamic elements as necessary. A detailed description of out proposed methodology is available upon request.

EXHIBIT 2
BUSINESS ASSOCIATE AGREEMENT AND SERVICE LEVEL AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT (hereinafter agreement) is between Tennessee Department of Health (hereinafter Covered Entity) and University of Tennessee **(CONTRACT # 34301-29219)** (hereinafter Business Associate). Covered Entity and Business Associate may be referred to herein individually as "Party" or collectively as "Parties."

BACKGROUND

Covered Entity acknowledges that it is subject to the Privacy Rule (45 C.F.R. Parts 160 and 164) promulgated by the United States Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191.

Business Associate acknowledges that effective February 17, 2010, the American Recovery and Reinvestment Act of 2009 (Pub. L.111-5), pursuant to Title XIII of Division A and Title IV of Division B, entitled the "Health Information Technology for Economic and Clinical Health" (HITECH) Act, which modifies the HIPAA Privacy and Security Rules, subjects and obligates the Business Associate to protect patient health information to the same extent and manner as the Covered Entity under the Privacy Rule (45 C.F.R. Parts 160 and 164) promulgated by the United States Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191. 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316 shall apply to a business associate of a covered entity in the same manner that these sections apply to the covered entity.

In the course of executing Service Contracts, Business Associate may come into contact with, use, or disclose Protected Health Information (PHI) (defined in Section 1.7 below). Said Service Contracts are hereby incorporated by reference and shall be taken and considered as a part of this document the same as if fully set out herein. In accordance with the federal privacy regulations set forth at 45 C.F.R. Part 160 and Part 164, Subparts A and E, which require Covered Entity to have a written contract with each of its Business Associates, the Parties wish to establish satisfactory assurances that Business Associate will appropriately safeguard PHI and, therefore, execute this Agreement.

1. DEFINITIONS

1.1. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 C.F.R. §§ 160.103, 164.304, 164.501 and 164.504.

1.2. "Breach" shall mean the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of the protected health information except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. 42 U.S.C.A. § 17921.

1.3. "Breach of the security system" under T.C.A. § 47-18-2107 means unauthorized acquisition of unencrypted computerized data that materially compromises the security of confidentiality or integrity of personal information maintained by the information holder.

1.4. "Designated Record Set" shall have the meaning set out in its definition at 45 C.F.R. § 164.501.

1.5. "Electronic Health Record" shall have the same meaning as set forth in the HITECH Act; "Electronic Protected Health Information" shall have the same meaning as set forth in 45 C.F.R. § 160.103, limited to the information that the Business Associate creates, receives, maintains, or transmits for or on behalf of the Covered Entity.

1.6. "Health Care Operations" shall have the meaning set out in its definition at 45 C.F.R. § 164.501.

1.7. “Individual” shall have the same meaning as the term “individual” in 45 C.F.R. § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

1.8. “Information Holder” means any person or business that conducts business in this state, or any agency of the state of Tennessee or any of the political subdivisions, that owns or stores computerized data that includes personal information. T.C.A. § 47-18-2107(a)(2).

1.9. “Personal Information” means an individual’s first name or first initial and last name, in combination with any one (1) or more of the following data elements, when either the name or the data elements are not encrypted: social security number, drivers license number, or account number, credit or debit card number; in combination with required security code, access code, or password that would permit access to an individual’s financial account. T.C.A. § 47-18-2107(a)(3)(A)

1.10. “Privacy Officer” shall have the meaning as set out in its definition at 45 C.F.R. § 164.530(a) (1).

1.11. “Privacy Rule” shall mean the Standards for Privacy for Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, subparts A and E.

1.12. “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 C.F.R. § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

1.13. “Required By Law” shall have the same meaning as the term “required by law” in 45 C.F.R. § 164.501.

1.14. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his/her designee.

1.15. “Security Event” shall mean an immediately reportable subset of security incidents which would include:

a) a suspected penetration of Business Associate’s information system of which the Business Associate becomes aware but for which it is not able to verify within FORTY-EIGHT (48) HOURS (of the time the Business Associate became aware of the suspected incident) that PHI or other confidential data was not accessed, stolen, used, disclosed, modified, or destroyed;

b) any indication, evidence, or other security documentation that the Business Associate’s network resources, including, but not limited to, software, network routers, firewalls, database and application servers, intrusion detection systems or other security appliances, may have been damaged, modified, taken over by proxy, or otherwise compromised, for which Business Associate cannot refute the indication within FORTY-EIGHT (48) HOURS of the time the Business Associate became aware of such indication;

c) a breach of the security of the Business Associate’s information system(s)(see definition 1.3 above), by unauthorized acquisition, including, but not limited to, access to or use, disclosure, modification or destruction, of unencrypted computerized data and which incident materially compromises the security, confidentiality, or integrity of PHI; and/or

d) the unauthorized acquisition, including, but not limited to, access to or use, disclosure, modification or destruction, of unencrypted PHI or other confidential information of the covered Entity by an employee or authorized user of Business Associate’s system(s) which

materially compromises the security, confidentiality, or integrity of PHI or other confidential information of the Covered Entity.

e) a security incident involving 500 or more patients shall be reported to HHS immediately and a security incident involving less than 500 patients shall be reported to HHS annually.

If data acquired (including. but not limited, to access to or use, disclosure, modification or destruction of such data) is in encrypted format but the decryption key which would allow the decoding of the data is also taken, the parties shall treat the acquisition as a breach for purposes of determining appropriate response.

1.16. "Security Incident" shall mean the attempt or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

1.17. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information" at 45 C.F.R. Parts 160 and 164, Subparts A and C.

1.18. "Services Agreement" shall mean any present or future agreements, either written or oral, between Covered Entity and Business Associate under which Business Associate provides services to the covered entity which involves the use or disclosure of Protected Health Information. The services Agreement is amended by and incorporates the terms of the business associate agreement.

1.19. "Unsecured Protected Health Information" is protected health information that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under 42 U.S.C.A. § 17932(h)(2) decoding of the data is also taken, the parties shall treat the acquisition as a breach for purposes of determining appropriate response.

2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE (PRIVACY RULE)

2.1. Business Associate agrees to fully comply with the requirements under the Privacy Rule applicable to "business associates," as that term is defined in the Privacy Rule and not use or further disclose Protected Health Information other than as permitted or required by this Agreement, Service Contracts as required by law. In case of any conflict between this Agreement and Service Contracts, this Agreement shall govern.

2.2. Business Associate agrees to implement administrative, including policies, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any PHI, including EPHI, that it creates, receives, maintains, or that it transmits on behalf of the covered entity to prevent use or disclosure of PHI other than as provided for by this Agreement. Said safeguards shall include, but are not limited to, requiring employees to agree to use or disclose PHI only as permitted or required by this Agreement and taking related disciplinary actions for inappropriate use or disclosure as necessary.

2.3. Business Associate shall, following a breach of unsecured PHI, as defined in the HITECH Act, immediately notify the Covered Entity pursuant to the terms of 45 C.F.R. § 164.410, cooperate in the Covered Entity's analysis procedures, including risk assessment, if requested. A breach shall be treated as discovered by the Business Associate as of the first day on which such breach is known or should have been known or, by exercising reasonable diligence, would have been known to Business Associate. Business Associate will provide notification to the Covered Entity without unreasonable delay and in no event later than twenty-four (24) hours of any suspected or actual breach of security, intrusion, or unauthorized use or disclosure. Such notification will contain the elements required in 45 C.F.R. § 164.410; and

2.4. Business Associate shall, pursuant to the HITECH Act and its implementing regulations, comply with all additional applicable requirements of the Privacy Rule, including those contained in 45 C.F.R. §§ 164.502(e) and 164.504(e)(1)(ii), at such time as the requirements become applicable to Business Associates. Business Associate will not accept payment in exchange for PHI, subject to the exceptions contained in the HITECH Act, without a valid authorization from the applicable patient/individual. Business associate shall not engage in any communication which might be considered marketing under the HITECH Act. Further, business Associate shall, pursuant to the HITECH Act and its implementing regulations, comply with applicable requirements of the Security Rule, contained in 45 C.F.R. §§ 164.308, 164.310, 164.312 and 164.316, at such time as the requirements are applicable to Business Associates.

2.5. Business Associate shall within ten (10) days of a written request from the Covered Entity and its agents or subcontractors allow the Covered Entity to conduct a reasonable inspection of the facility, systems, books, records agreements, policies and procedures relating to the use, or disclosure of protected health information pursuant to this Agreement for the purpose of monitoring compliance with the terms of this Agreement.

2.6. Business Associate shall require any agent, including a subcontractor, to whom it provides PHI received from, created or received by, Business Associate on behalf of Covered Entity or that carries out any duties for the Business Associate involving the use, custody, disclosure, creation of, or access to PHI, to agree, by written contract with Business Associate, to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

2.7. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement. Business Associate agrees to require its employees, agents, and subcontractors to immediately report, to Business Associate, any use or disclosure of Protected Health Information in violation of this Agreement, and to report to Covered Entity any use or disclosure of the PHI not provided by or agreed upon in this Agreement.

2.8. If Business Associate receives PHI from Covered Entity in a Designated Record Set, then Business Associate agrees to provide access, at the request of Covered Entity, to PHI in a Designated Record Set, to Covered Entity or, as directed by covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524, provided that Business Associate shall have at least thirty (30) days from Covered Entity's notice to provide access to, or deliver such information.

2.9. If Business Associate receives Protected Health Information from Covered Entity in a Designated Record Set, then Business Associate agrees to make any amendments to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to the 45 C.F.R. §164.526 at the request of Covered Entity or an Individual, and in the time and manner designated by Covered Entity, provided that Business Associate shall have at least thirty (30) days from Covered Entity notice to make an amendment.

2.10. Business Associate agrees to make its internal practices, books, and records including policies and procedures and Protected Health Information, relating to the use and disclosure of PHI received from, created by or received by Business Associate on behalf of, Covered Entity available to the Covered Entity or to the Secretary of the United States Department of Health in Human Services or the Secretary's designee, in a time and manner designated by the Covered Entity or the Secretary, for purposes of determining Covered Entity's or Business Associate's compliance with the Privacy Rule.

2.11. Business Associate agrees to document disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for

an accounting of disclosure of PHI in accordance with 45 C.F.R. §164.528.

2.12. Business Associate agrees to provide Covered Entity or an Individual, in time and manner designated by Covered Entity, information collected in accordance with this Agreement, to permit Covered Entity to respond to a request by an Individual for and accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528, provided that Business Associate shall have at least thirty (30) days from Covered Entity notice to provide access to, or deliver such information which shall include, at minimum, (a) date of the disclosure; (b) name of the third party to whom the Protected Health Information was disclosed and, if known, the address of the third party; (c) brief description of the disclosed information; and (d) brief explanation of the purpose and basis for such disclosure.

2.13. Business Associate agrees it must limit any use, disclosure, or request for use or disclosure of PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request in accordance with the requirements of the Privacy Rule. Business Associate understands and agrees that the definition of “minimum necessary” has not been established by HHS guidance and shall keep itself informed of guidance issued by the Secretary with respect to what constitutes “minimum necessary.”

2.14. Business Associate agrees it must use reasonable efforts to limit any use, disclosure, or request for use of disclosure of PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request in accordance with the requirements of the Privacy Rule.

2.15. Covered Entity may, pursuant to the Privacy Rule, reasonably rely on any requested disclosure as the minimum necessary for the stated purpose when the information is requested by Business Associate.

2.16. Business Associate acknowledges that if Business Associate is also a covered entity, as defined by the Privacy Rule, Business Associate is required, independent of Business Associate's obligations under this Agreement, to comply with the Privacy Rule's minimum necessary requirements when making any request for PHI from Covered Entity.

2.17. Business Associate agrees to adequately and properly maintain all Protected Health Information received from, or created or received on behalf of, Covered Entity, document subsequent uses and disclosures of such information by Business Associate as may be deemed necessary and appropriate by the Covered Entity, and provide Covered Entity with reasonable access to examine and copy such records and documents during normal business hours of Business Associate.

2.18. Business Associate agrees that Covered Entity may at any time review Business Associate's privacy policies and procedures to determine whether they are consistent with Covered Entity's policies, procedures, and privacy practices, and shall promptly notify Business Associate in writing regarding any modifications Covered Entity may reasonably believe are needed in order to meet Covered Entities requirements.

2.19. If Business Associate receives a request from an individual for a copy of the individual's Protected Health Information, and the Protected Health Information is in the sole possession of the Business Associate, Business Associate will provide the requested copies to the individual and notify the Covered Entity of such action. If Business Associate receives a request for PHI in the possession of the Covered Entity, or receives a request to exercise other individual rights as set forth in the Privacy Rule, Business Associate shall notify Covered Entity of such request and forward the request to Covered Entity. Business Associate shall then assist Covered Entity in responding to the request.

2.20. Business Associate agrees to fully cooperate in good faith with and to assist Covered Entity in

complying with the requirements of the Privacy Rule.

3. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE (Security Rule)

3.1. Business Associate agrees to fully comply with the requirements under the Security Rule applicable to "business associates" as such terms is defined in the Security Rule. In case of any conflict between this Agreement and Service Contracts, this agreement shall govern.

3.2. Business Associate Agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of the covered entity as required by the Security Rule. This includes specifically, but not limited to, the utilization of technology commercially available at the time to the Business Associate to protect the Covered Entity's PHI against any reasonably anticipated threats or hazards The Business Associate understands that it has an affirmative duty to perform a regular review or assessment of security risks, conduct active risk management and supply best efforts to assure that only authorized persons and devices access its computing systems and information storage, and that only authorized transactions are allowed. The Business Associate will maintain appropriate documentation of its compliance with the Security Rule.

3.3. Business Associate shall ensure that any agent, including a subcontractor, to whom it provides electronic PHI received from, maintained, or created for Covered Entity or that carries out any duties for the Business Associate involving the use, custody, disclosure, creation of, or access to PHI supplied by Covered Entity, shall execute a bilateral contract (or the appropriate equivalent if the agent is a government entity) with Business Associate, incorporating the same restrictions and conditions in this Agreement with Business Associate regarding PHI.

3.4. Tennessee Consumer Notice of System Breach. Business Associate understands that the Covered Entity is an "information holder" (as may be Business Associate) under the terms of T.C.A. § 47-18-2107, and that in the event of a breach of the Business Associate's security system as defined by that statute and Definition 1.7 of this agreement, the Business Associate shall indemnify and hold the Covered Entity harmless for expenses and/or damages related to the breach. Such obligations shall include, but is not limited to, the mailed notifications to any Tennessee resident whose personal information is reasonably believed to have been acquired by an unauthorized individual. In the event that the Business Associate discovers circumstances requiring notification of more than a thousand (1,000) persons at one time, the person shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. §1681a, of the timing distribution and content of the notices. Substitute notice as defined T.C.A. § 47-18-2107(e)(2) and (3), shall not be permitted except as approved in writing in advance by the Covered Entity. The parties agree that PHI includes data elements in addition to those included by "personal information" under T.C.A. § 47-18-2107, and agree that Business Associate's responsibilities under this paragraph shall include all PHI and PII.

3.5. Reporting of Security Incidents. The Business Associate shall track all security incidents as defined by HIPAA. The Business Associate shall reasonably use its own vulnerability assessment of damage potential and monitoring to define levels of Security Incidents and responses for Business Associate's operations. However, the Business Associate shall expediently notify the Covered Entity's Privacy Officer of any Security Incident which would constitute a Security Event as defined by this Agreement, including any "breach of the security of the system" under T.C.A. § 47-18-2107, in a preliminary report within two (2) business days of any unauthorized acquisition including, but not limited to, use, disclosure, modification, or destruction of PHI by an employee or otherwise authorized user of its system of which it becomes aware with a full report of the incident not less than five (5) business days of the time it became aware of the incident.

3.5.1 Business Associate shall identify in writing key contact persons for administration, data processing, Marketing, Information Systems and Audit Reporting within thirty (30) days of execution of this Agreement. Business Associate shall notify Covered Entity of any reduction of in-house staff persons during the term of this Agreement in writing within ten (10) business days.

3.6. Contact for Security Event Notice. Notification for the purposes of Sections 2.7, 3.4 and 3.5 shall be in writing made by certified mail or overnight parcel within two (2) business days of the event, with supplemental notification by facsimile and/or telephone as soon as practicable, to the designated Privacy Official of the Covered Entity in accordance to 8.5 Notices and Communications.

3.7. Security Compliance Review upon Request. Business Associate agrees to make its internal practices, books, and records, including policies and procedures relating to the security of electronic PHI received from, created by or received by Business Associate on behalf of Covered Entity, available to the Covered Entity or to the Secretary of the United States Department of Health in Human Services or the Secretary's designee, in a time and manner designated by the requester, for purposes of determining Covered Entity's or Business Associate's compliance with the Security Rule.

3.8. Cooperation in Security Compliance. Business Associate agrees to fully cooperate in good faith and to assist Covered Entity in complying with the requirements of the Security Rule.

4. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

4.1. Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in Service Contracts, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity.

4.2. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information as required for Business Associate's proper management and administration or to carry out the legal responsibilities of the Business Associate. In the event a party to this Agreement receives a subpoena, court order, or other demand for the information in this Agreement, the receiving party shall immediately inform the other party in writing concerning the demand.

4.3. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are required by law, or provided that, if Business Associate discloses any Protected Health Information to a third party for such a purpose, Business Associate shall enter into a written agreement with such third party requiring the third party to: (a) maintain the confidentiality of Protected Health Information and not to use or further disclose such information except as Required By Law or for the purpose for which it was disclosed, and (b) notify Business Associate of any instances in which it becomes aware in which the confidentiality of the Protected Health Information is breached.

4.4. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 C.F.R. § 164.504(e)(2)(I)(B).

5. OBLIGATIONS OF COVERED ENTITY

5.1. Covered Entity shall provide Business Associate with the notice of privacy practices that Covered

Entity produces in accordance with 45 C.F.R. § 164.520, as well as any changes to such notice.

5.2. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses.

5.3. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use of Protected Health Information.

6. PERMISSIBLE REQUESTS BY COVERED ENTITY

6.1. Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

7. TERM AND TERMINATION

7.1. Term. This Agreement shall be effective as of the date on which it is signed by both parties and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, Section 7.3 below shall apply.

7.2. Termination for Cause.

7.2.1. This Agreement authorizes and Business Associate acknowledges and agrees Covered Entity shall have the right to immediately terminate this Agreement and Service Contracts in the event Business Associate fails to comply with, or violates a material provision of, requirements of the Privacy Rule or this Agreement.

7.2.2. Upon Covered Entity's knowledge of a material breach by Business Associate,

7.2.2.1. Covered Entity shall, whenever practicable, provide a reasonable opportunity for Business Associate to remedy the breach or end the violation.

7.2.2.2. If Business Associate has breached a material term of this Agreement and remedy is not possible or if Business Associate does not remedy a curable breach or end the violation within a reasonable time as specified by, and at the sole discretion of, Covered Entity, Covered Entity may immediately terminate this Agreement and Service Contracts.

7.2.2.3. If neither remedy nor termination is feasible, Covered Entity shall report the violation to the Secretary of the United States Department of Health in Human Services or the Secretary's designee.

7.3. Effect of Termination.

7.3.1. Except as provided in Section 7.3.2 below, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of, Covered Entity. This provision shall apply to Protected Health Information that is in the

possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

7.3.2. In the event that Business Associate determines that returning or destroying the Protected Health Information is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction unfeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is unfeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction unfeasible, for so long as Business Associate maintains such Protected Health Information.

8. MISCELLANEOUS

8.1. Regulatory Reference. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

8.2. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act, Public Law 104-191. Business Associate and Covered Entity shall comply with any amendment to the Privacy Rule, the Health Insurance Portability and Accountability Act, Public Law 104-191, and related regulations upon the effective date of such amendment, regardless of whether this Agreement has been formally amended.

8.3. Survival. The respective rights and obligations of Business Associate under Section 7.3. of this agreement shall survive the termination of this Agreement.

8.4. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy Rule.

8.5. Notices and Communications. All instructions, notices, consents, demands, or other communications required or contemplated by this Agreement shall be in writing and shall be delivered by hand, by facsimile transmission, by overnight courier service, or by first class mail, postage prepaid, addressed to the respective party at the appropriate facsimile number or address as set forth below, or to such other party, facsimile number, or address as may be hereafter specified by written notice.

COVERED ENTITY:

Tennessee Department of Health
Privacy Officer
710 James Robertson Parkway (5th Floor) Nashville, TN 37243
Email: Phil.Wilson@tn.gov
Telephone: 615-741-5229
Fax: 615-253-3926

Tennessee Department of Health
Mike Moak, Security Officer
710 James Robertson Parkway (6th Floor) Nashville, TN 37243
Email: Mike.Moak@tn.gov
Telephone: 615-741-0899
Fax: 615-253-3926

BUSINESS ASSOCIATE:
University of Tennessee
Name and Title:
Address
Email:
Telephone:
Fax:

All instructions, notices, consents, demands, or other communications shall be considered effectively given as of the date of hand delivery; as of the date specified for overnight courier service delivery; as of three (3) business days after the date of mailing; or on the day the facsimile transmission is received mechanically by the facsimile machine at the receiving location and receipt is verbally confirmed by the sender.

8.6. Strict Compliance. No failure by any Party to insist upon strict compliance with any term or provision of this Agreement, to exercise any option, to enforce any right, or to seek any remedy upon any default of any other Party shall affect, or constitute a waiver of, any Party's right to insist upon such strict compliance, exercise that option, enforce that right, or seek that remedy with respect to that default or any prior, contemporaneous, or subsequent default. No custom or practice of the Parties at variance with any provision of this Agreement shall affect, or constitute a waiver of, any Party's right to demand strict compliance with all provisions of this Agreement.

8.7. Severability. With respect to any provision of this Agreement finally determined by a court of competent jurisdiction to be unenforceable, such court shall have jurisdiction to reform such provision so that it is enforceable to the maximum extent permitted by applicable law, and the Parties shall abide by such court's determination. In the event that any provision of this Agreement cannot be reformed, such provision shall be deemed to be severed from this Agreement, but every other provision of this Agreement shall remain in full force and effect.

8.8. Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Tennessee.

8.9. Compensation. There shall be no remuneration for performance under this HIPAA Business Associate Agreement except as specifically provided by, in, and through, contractual relationships referenced herein.

IN WITNESS WHEREOF,

TENNESSEE DEPARTMENT OF HEALTH:

Lisa Piercey MD-LO

Digitally signed by Lisa Piercey MD-LO
DN: cn=Lisa Piercey MD-LO, o, ou, email=Lindsay.R.Oliveras@tn.gov, c=US
Date: 2019.09.12 09:36:54 -05'00'

LISA PIERCY, MD, MBA, FAAP, COMMISSIONER **Date**

BUSINESS ASSOCIATE LEGAL ENTITY NAME:

NAME AND TITLE **Date**